臺北城市科技大學個人資料檔案安全維護計畫

民國 114 年 6 月 30 日 113 學年度第 2 學期第 10 次行政會議通過

一、依據教育部 103 年 8 月 21 日臺教高通字第 1030117307B 號令訂定「私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法」發布施行。

二、目的

臺北城市科技大學（以下簡稱本校）為落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損或洩漏，與業務終止後個人資料處理事項，特訂定本校個人資料檔案安全維護計畫（以下簡稱本計畫）。

三、適用範圍

本校之個人資料管理其範圍應涵蓋全校，基於特定目的範圍內之所有之教育或訓練行政、學生資料管理、人事管理及內部控制事項等，包含所有之教職員工及學生之個人資料蒐集、處理、利用及國際傳輸。

四、界定個人資料、風險評估及管理機制

（一） 組織背景

1. 本校主管機關為教育部。

2. 蒐集、處理或利用之個人資料主要為履行法定義務。

（二） 本校得指定或設管理單位，或指定專人負責個人資料檔案。

（三） 組織適用之特定目的

1.目前本校持有個人資料之特定目的分為以下幾類：

002 人事管理

063 非公務機關依法定義務所進行個人資料之蒐集處理及利用

069 契約、類似契約或其他法律關係事務

109 教育或訓練行政

110 產學合作

136 資（通）訊與資料庫管理

146 圖書館管理

157 調查、統計與研究分析

158 學生(員)資料管理(含畢、結業生)

159 學術研究

160 憑證業務管理

2.未來若有任何單位因非上述所列之特定目的或在上述特定目的外需蒐集、處理或利用個人資料，需再行說明新蒐集、處理或利用之特定目的或特定目的外蒐集、處理或利用之原因。

3.本校應定期清查所保有之個人資料現況。經檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用

等適當之處置。

（四） 向當事人蒐集個人資料時，除法律明文規定外，需經當事人同意並明確告知蒐集目的、個人資料之類別、利用期間、地區、對象及方式。

（五） 界定個人資料範圍

1. 本校對於個人資料之定義：「個人資料保護法」第 2 條所規範之 19 項個人資料以及「個人資料保護法之特定目的及個人資料之類別」所規範之個人資料類別。
2. 本校蒐集、處理及利用之個人資料類別，依據「個人資料保護法之特定目的及個人資料之類別」分類如下：
   - C001 辨識個人者：姓名、住址、電話、身分證字號、護照號碼、學生證號、教職員編號、照片等。
   - C002 辨識財務者：金融機構帳號、薪資轉帳資料、保險資料、退撫基金資訊。
   - C003 政府資料中之辨識者：戶籍資料、兵役資料、納稅資料。
   - C011 個人描述：性別、出生年月日、國籍、婚姻、學歷、家庭狀況等。
   - C021 學校紀錄：學籍資料、修課紀錄、考試成績、獎懲紀錄、畢業資格審查等。
   - C023 職業專長：證照、語言能力、專業技能、研究成果。
   - C024 就業歷程：工作經驗、任職紀錄、在校兼任紀錄。
   - C035 休閒與興趣：參與活動、社團經驗等。
   - C036 生活型態：住宿資料、校內交通使用等。
   - C038 職業操守：教師或職員違紀紀錄。
   - C061 現行之違法行為：若涉違規調查程序（如性平、校安通報）所產生之資料。
   - C073 健康紀錄（特種個資）：健康檢查報告、疫苗接種資料、心理測驗結果（需書面同意）。
   - C081 學生資料：畢業證書、學業歷程資料。
   - C132 未分類之資料：照片影像（校園攝影、出席活動）、問卷等非上述類型。
3. 「特種個人資料」之蒐集、處理與利用：本校依照「學校衛生法」規定，學校應建立學生健康管理制度；健康檢查及疾病檢查結果，應載入學籍資料。依「勞工安全衛生法」規定：可蒐集、處理與利用「員工」之「健康檢查」及「醫療」相關資訊。特種個人資料得經當事人書面同意蒐集、處理或利用。
4. 本校需進行全面性之個人資料盤點，範圍包括本校目前持有之

個人資料、本校受委託蒐集、處理或利用之個人資料以及本校委託外部機關蒐集、處理或利用之個人資料皆屬之。

（六） 風險評估及管理機制

1. 本校所有與個人資料相關之流程與檔案資料之管理皆必須進行風險評估。
2. 評估作業包含辨識個人資料流（蒐集、保存、處理、傳輸、銷毀）各階段的潛在風險。
3. 依衝擊程度（高/中/低）與發生機率（高/中/低）交叉評級，作為風險矩陣，對高風險等級之作業，應提出具體改善計畫。
4. 圖資處校資組為主責單位，負責規劃評估表格、召集會議、彙整報告，並保存相關記錄。

五、個人資料安全

（一） 個人資料檔案之存取，應釐定使用範圍及使用權限，並設置帳號、密碼且不與他人共用。

（二） 個人資料檔案儲存在個人電腦者，應在該個人電腦設置開機密碼、螢幕保護程式密碼及相關安全措施。

（三） 個人資料檔案使用完畢，應即退出應用系統，不得留置在電腦顯示畫面上。

（四） 應定期更換密碼，同一密碼使用期限最長應不超過 6 個月，並應儘量避免重複或循環使用舊的密碼。

（五） 個人資料檔案應建立保存期限，並確實辦理保存與銷毀。

（六） 以網際網路蒐集、處理、利用及國際傳遞個人資料時，應採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

（七） 本校應訂定應變機制，應自第一項個人資料被竊取、洩露、竄改或其他侵害事故發現時，應迅速處理以保護當事人之權益，並於 72 小時內，通報主管機關。

（八） 本校委託他人蒐集、處理或利用個人資料之全部或一部份時，應依個人資料保護法施行細則第八條規定對受託者為適當之監督，並明確約定相關監督事項及方式。

（九） 本校利用個人資料為宣傳、推廣或行銷時，應明確告知當事人其所屬本校活動名稱及個人資料來源。本校於首次利用個人資料為宣傳、推廣或行銷時，應提供當事人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；當事人表示拒絕宣傳、推廣或行銷後，應立即停止利用其個人資料宣傳、推廣或行銷，並周知所屬人員。

（十） 本校於當事人行使個人資料保護法第三條規定，當事人可行使以

下權利時，得採取相關方式辦理：

1.查詢或請求閱覽。

2.請求製給複製本。

3.請求補充或更正。

4.請求停止蒐集、處理及利用。

5.請求刪除。

（十一）本校業務終止後，其保有之個人資料之處理方式及留存紀錄如下：

1. 銷毀：可使用碎紙機、物理破壞或其他不可逆之實體破壞方法，經審核奉准後，於時限內實施，進行前項個人資料銷毀處理時，應記載處理之時間、地點，並留存相關記錄。
2. 移轉：業務移轉經審核奉准，於時限內實施移轉作業，並記錄移轉之文件、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。
3. 刪除、停止處理或利用個人資料：業務終止後經審核奉准，於時限內實施資料刪除、停止處理或利用作業，並留存時間或地點等記錄。

（十二）本校於個人資料蒐集、處理及利用時依個資法第 8 條要求，明確告知蒐集之目的、類別、利用之期間、地區、對象及方式。

（十三）當事人得自由選擇提供個人資料時，不提供將對其權益之影響：當事人若選擇不提供個人資料，可能會影響其在本校的學籍、薪資、考試等相關行政事宜，並可能無法參與部分學術或行政服務。

（十四）本校對於個人資料蒐集、處理及利用應符合個人資料保護法第十九條及第二十條規定，並應定期或不定期對其所屬人員施以教育訓練或認知宣導，使其明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。

六、個人資料稽核

（一） 建立個人資料檔案稽核制度，指定專人定期或不定期稽核個人資料檔案管理情形，並針對控管結果之不符合事項與潛在風險，規劃改善及預防措施。執行改善及預防措施時，應完成以下事項：

1. 確認不符合事項根本原因。
2. 提出改善及預防措施。
3. 紀錄執行結果。

（二） 以電腦處理個人資料時，應核對個人資料之輸入、輸出、編輯或更正是否與原檔案相符。

（三） 稽核人員得調閱有關資料，並請相關人員提供說明。

七、設備管理

（一） 建置個人資料之有關電腦設備，資料管理單位應隨時保持系統更新。

（二） 非有必要，不得任意移動處理個人資料之電腦設備，若有調動需求，應保留相關紀錄。

（三） 建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。

（四） 指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。

（五） 電腦設備進行報廢或汰換前，應確實將機密性、敏感性及個人資料予以刪除，以確保任何機密性、敏感性、個人隱私之資料不外流。

八、其他安全維護事項

（一） 處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料列冊移交，接收人應另行設定密碼，以利管理。

（二） 教職員離職後，其離職人員曾接觸過之密碼均需作適當之調整。

（三） 其他未詳述作法將參閱本校 ISMS 資訊安全管理制度執行。

九、本校個人資料保護聯絡窗口：圖書資訊處校務資訊組，聯絡信箱：imt@tpcu.edu.tw

十、本計畫經行政會議通過，校長核定後公布實施。